

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.



## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<b>(51) International Patent Classification:</b> <b>G06F 17/60, G06F 1/00,</b> <b>H04L 29/06</b>	<b>A1</b>	<b>(11) International Publication Number:</b> <b>WO 00/62232</b> <b>(43) International Publication Date:</b> 19 October 2000 (19.10.2000)
<b>(21) International Application Number:</b> PCT/US00/09774 <b>(22) International Filing Date:</b> 12 April 2000 (12.04.2000) <b>(30) Priority Data:</b> 09/546,813 11 April 2000 (11.04.2000) US 60/128,846 12 April 1999 (12.04.1999) US <b>(60) Parent Application or Grant</b> DIGITAL MEDIA ON DEMAND, INC. (DMOD, INC.) [/]; O RAUBER, Ty, P. [/]; O. HEADRICK, Samuel, P. [/]; O. CAMPBELL, Rod, I. [/]; O. FASULLO, Brett, P. [/]; O. HESTER, Stephen, D. [/]; O. MIRABITO, A., Jason ; O.	<b>Published</b>	
<b>(54) Title: SECURE ELECTRONIC COMMERCE SYSTEM</b> <b>(54) Titre: SYSTEME DE COMMERCE ELECTRONIQUE SUR</b>		
<b>(57) Abstract</b> <p>A secure electronic commerce system and method provides for the distribution of artistic works in electronic formats. The system includes a server system which permits the author or owner of a work to upload and store an electronic copy of the work and allows a plurality of client systems to access the server system to download encrypted copies of the work. The server system can also include an electronic commerce system which enables a client system to transfer value from a credit account or a debit account to an account associated with the server system in exchange for permission to download works. The server system includes an encryption system which stores a unique key for each client system and uses the key to encrypt each work download to a corresponding client system. Each client system includes an encryption system and a unique key which enables only that system to decrypt the work to all a consumer to use the work. The unique key can also be used to verify the identity of the client system.</p> <b>(57) Abrégé</b> <p>L'invention concerne un système et un procédé de commerce électronique sûr permettant la distribution d'oeuvres d'art en formats électroniques. Ce système comprend un système serveur qui permet à l'auteur ou au propriétaire d'une oeuvre de télécharger et de mémoriser une copie électronique de l'oeuvre et à une pluralité de système clients d'accéder au système serveur afin de télécharger des copies de l'oeuvre sous forme chiffrée. Le système serveur peut en outre comprendre un système de commerce électronique qui permet à un système client de transférer un montant à partir d'un compte de crédit ou de débit sur un compte associé au système serveur en échange d'une autorisation de téléchargement des oeuvres. Ce système serveur comprend un système de chiffrement dans lequel une clé unique est enregistrée pour chaque système client, et utilise cette clé pour chiffrer chaque téléchargement d'oeuvre à l'intention du système client correspondant. Chaque système client comprend un système de chiffrement et une clé unique qui permet uniquement à ce système de déchiffrer l'oeuvre de manière que le consommateur puisse utiliser l'oeuvre. Cette clé unique peut également servir à vérifier l'identité du système client.</p>		

PCT

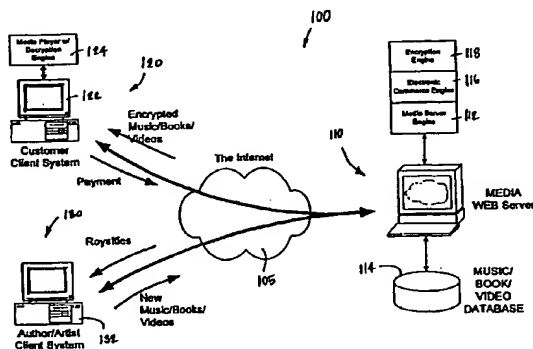
WORLD INTELLECTUAL PROPERTY ORGANIZATION  
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : <b>G06F 17/60, H04L 29/06, G06F 1/00</b>		<b>A1</b>	(11) International Publication Number: <b>WO 00/62232</b>
			(43) International Publication Date: 19 October 2000 (19.10.00)
(21) International Application Number: <b>PCT/US00/09774</b>		(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: <b>12 April 2000 (12.04.00)</b>		<b>Published</b> <i>With International search report. Before the expiration of the time limits for amending the claims and to be republished in the event of the receipt of amendments.</i>	
(30) Priority Data: 60/128,846 12 April 1999 (12.04.99) US 09/546,813 11 April 2000 (11.04.00) US			
(71) Applicant: DIGITAL MEDIA ON DEMAND, INC. (DMOD, INC.) [US/US]; 244 Brighton Avenue, Allston, MA 02134 (US).			
(72) Inventors: RAUBER, Ty, P.; 1259 Commonwealth Avenue #5, Allston, MA 02134 (US). HEADRICK, Samuel, P.; 499 Park Drive #1, Boston, MA 02215 (US). CAMPBELL, Rod, I.; 499 Park Drive #1, Boston, MA 02215 (US). FASULLO, Brett, P.; 1259 Commonwealth Avenue #6, Allston, MA 02134 (US). HESTER, Stephen, D.; 1259 Commonwealth Avenue #5, Allston, MA 02134 (US).			
(74) Agent: MIRABITO, A., Jason; Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C., One Financial Center, Boston, MA 02111 (US).			

(54) Title: SECURE ELECTRONIC COMMERCE SYSTEM



(57) Abstract

A secure electronic commerce system and method provides for the distribution of artistic works in electronic formats. The system includes a server system which permits the author or owner of a work to upload and store an electronic copy of the work and allows a plurality of client systems to access the server system to download encrypted copies of the work. The server system can also include an electronic commerce system which enables a client system to transfer value from a credit account or a debit account to an account associated with the server system in exchange for permission to download works. The server system includes an encryption system which stores a unique key for each client system and uses the key to encrypt each work download to a corresponding client system. Each client system includes an encryption system and a unique key which enables only that system to decrypt the work to all a consumer to use the work. The unique key can also be used to verify the identity of the client system.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

## Description

5

10

15

20

25

30

35

40

45

50

55

1  
SECURE ELECTRONIC COMMERCE SYSTEM

## COPYRIGHT NOTICE

Copyright, 1998, 1999, DMOD, Inc. A portion of the disclosure of this patent document contains material which is subject to copyright protection. The copyright owner has no objection to reproduction by anyone of the patent document or the patent disclosure, as it appears in the U.S. Patent and Trademark Office patent file or records, but otherwise reserves all copyright rights whatsoever.

## CROSS-REFERENCE TO RELATED APPLICATIONS

This application is related to and claims the benefit of U.S. Provisional Application Serial No. 60/ 128,846, filed April 12, 1999, which is hereby incorporated by reference in its entirety.

## STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH

Not Applicable

## REFERENCE TO MICROFICHE APPENDIX

Not Applicable

## BACKGROUND OF THE INVENTION

This invention relates to secure methods and systems for conducting electronic commerce and the distribution of audio, video, and text works and, more particularly, to a method and system which utilizes encryption in a client-server environment to provide secure electronic commerce transactions and the encrypted distribution of audio, video and text works for value.

5 Traditionally, entertainment and artistic works such as music and movies, are distributed by incorporating a copy of the work in a medium from which the work, such as a song or a movie, can be heard or viewed using a device. For example, music is distributed on records, tapes and compact discs and movies are distributed on tapes and digital video disks. The technologies associated with these media have developed over time in order to permit very high quality reproductions of the original work.

15 The technology also exists to convert these works into digital data that can be stored in memory in a computer or distributed via a network. This technology permits the works to be stored on digital media such as compact discs ("CDs") and digital video disks ("DVDs"). One of the disadvantages of this technology is that in order to provide a high level of sound and video quality, the works require very large quantities of memory. For example, a four minute song recorded on a CD occupies approximately 40 Megabytes of digital data in its native format, thus limiting the number songs that can be contained on a single CD and making distribution of music using the present network infrastructure impractical.

35 Alternative technologies have been developed which enable that same four minute song to be stored in less than 4 Megabytes of digital data. One such technology, MPEG 1, audio layer 3, which is more commonly known as MP3, defines how digital audio can be stored and transmitted using computers and networks. Other standards and technologies currently exist and still others are being developed.

45 These digital media technologies allow a consumer to store music in non-volatile memory such as a harddisk drive in a personal computer and use a software program, applet or plugin, commonly referred to as a media player, to play the music using the multimedia resources of a personal computer. Well known media players for MP3 technologies include WinAmp available from NullSoft, Inc. of Sedona, Arizona and

5 Sonique available from Mediascience, Inc. of San Francisco, California. These products  
allow a user to play MP3 encoded audio on a personal computer. Other products, such as  
10 the Rio available from Diamond Multimedia, Inc. and the MPMan available from Saehan  
Information Systems, Inc. of Seoul, Korea, enable a consumer to store and play MP3  
15 encoded audio in a portable device. These electronic devices typically store the MP3  
encoded audio in a flash memory that allows non-volatile storage of the audio and allows  
the MP3 encoded audio to be erased or over written.

20 Digital medial technologies such as MP3 facilitate the ability to distribute audio  
and video via the current network infrastructure such as the internet. These technologies  
10 enable independent authors and artists to setup websites on the World Wide Web  
("WWW") to distribute their works and overcome conventional barriers to distribution,  
25 which typically require the author or artist to enter into an agreement with a third party  
organization, such as a publishing or recording company, to promote and distribute the  
author or artist's work. These technologies also provide a means for the unauthorized  
30 distribution of the work.  
15

35 In addition, there is no integrated system or infrastructure in place to enable music  
distributors, for example, to collect royalties on a per track (or per song) basis. Presently,  
music is distributed in album format which includes multiple tracks. There is no effective  
40 way to track which consumers were licensed which works. There is no effective way to  
20 verify the identity of consumer who is attempting download a copy of a work over a  
network such as the internet.

45 Accordingly, it is an object of this invention to provide an improved method and  
system for distributing audio, video and text works.



4

5 It is another object of the present invention to provide an improved method and  
system for distributing audio, video and text works which prevents the unauthorized  
distribution or redistribution of the works.

10 It is yet another object of the present invention to provide an improved method and  
5 system for managing the electronic commerce of the distribution of works and other goods  
or services over a network such as the internet.

#### SUMMARY OF THE INVENTION

20 The present invention is directed to a method and system for distributing goods and  
10 audio, video and text works over a network, such as the Internet. The method and system  
according to the invention allow for the transaction to occur in a secure manner which  
25 permits the distributor to verify the identity of the consumer (or customer) and impedes  
the unauthorized distribution of the works by the consumer (or customer) and third  
30 parties.

15 The system according to the present invention includes a server system which  
permits the owner of the work or the distributor to store and distribute the work over a  
35 network and a client system which is adapted to communicate with the server system to  
receive copies of the work over the network. The server system can include storage  
40 memory for storing copies of the works to be distributed or alternatively the server system  
20 can be adapted to access a storage facility which stores copies of the works, such as over a  
network or other data connection. The server system can also include an electronic  
45 commerce system which is adapted for receiving value (payment) from the consumer or  
customer and distributing that value to various parties for example the owner of the work  
and the authorized distributor of the work. The electronic commerce system can receive  
50 value from the consumer on either a credit basis (such as using a credit card account) or a  
25

55

5

5 debit basis (such as allowing consumers to purchase credits against which they may receive works). The server system can also include an encryption system which allows the distributor to uniquely encrypt the works distributed to a consumer. Thus, the works distributed to one consumer could be differently encrypted from the works distributed to another consumer. The server system can include an encryption key database which maintains a unique key for each consumer. The unique key can also serve to allow the distributor or retailer to verify the identity of the client system (and the consumer) and to uniquely encrypt the copy of the work or any other data that is transmitted to the client system (and the consumer).

10 The client system according to the present invention can be adapted to interface with the above described server system to transfer value from the consumer to the distributor (and the owner) and transfer a copy of the work to the consumer. The client system can include an encryption system which is uniquely adapted to decrypt the work distributed to the consumer in possession of the client system. In one embodiment, the client system can incorporate the unique key from the server system. The client system can include several unique keys from several different server systems.

35 The client system according to the present invention can be adapted to interface with the electronic commerce system of the above described server to facilitate the transfer of value and enable to the distributor or retailer to verify the identity of the client system and ultimately the consumer. In one embodiment, the server system maintains a unique encryption key which is embedded (or hard coded) into the client system. The server system can verify the identity of the client system by requesting the client system to transmit a predefined message, identification code, or electronic certificate which is encrypted using the key embedded in the client system. The server system can use the unique key stored in the key database to verify the encrypted message came from the

55

6

5 client that is registered in the database by decrypting the predefined message and  
comparing it to an expected value. The same message can include other information such  
as a credit card information (number and expiration date) or an authorization to debit an  
10 account (including an account number). Alternatively, other known identification  
5 verification methods can be used to verify the client system.

15 In another embodiment, a public key encryption system can be used to encrypt the  
work and any messages that are transferred between the server system and to the client  
system. In this embodiment, the system can further include a public key server which is  
20 adapted to transmit the server system's public key to the client and the client system's  
10 public key to the server system. Digital signatures can be used by both the client system  
and the server system to verify the identity of the other. Public key encryption systems  
25 are available from RSA Data Security, Inc. of San Mateo, California.

30 In one embodiment, the client system can also include a media player adapted to  
enable the consumer to use to the work as permitted by the owner, such as listen to an  
15 audio work, view a video work or read text in a manner similar to the way one would read  
a book. Alternatively, a separate media player could be used. As used herein, the client  
35 system can reside on a personal computer or the client system can be a combination of  
hardware and software that is configured or adapted to perform the functions described,  
40 such as a portable device similar to a portable tape or CD player.

20 In an alternative embodiment of the present invention, the client and server  
systems can be part of a universal electronic commerce system. In this embodiment, the  
45 client system can be a universal electronic commerce client to facilitate electronic  
transactions over a network such as the Internet. In this embodiment, the client can be  
embedded into a web browser or be a "plug-in" software module that provides additional  
50 functionality to a browser or other program. The universal electronic commerce system  
25

55

5 can include several server systems which can reside on a single system or be distributed  
over a network, such as a virtual private network or the internet. This embodiment can  
include a retailer or distributor server which is adapted to interface with the client to  
10 facilitate an electronic transaction with a consumer. The system can also include a key  
server which is adapted to manage the key database to transfer consumer keys to the  
15 retailer or distributor and transfer retailer or distributor keys to the consumer. In one  
embodiment, the key server is managed by an independent company, trusted industry  
organization, or the government. The system can further include a credit or debit account  
20 server which manages the various accounts, including the consumer account, the retailer  
account, the distribution account and the owner account. In one embodiment; the credit or  
25 debit account server can be managed by a credit card company, a bank or similar  
organization. Alternatively, the key distribution and credit/debit functions can be  
managed on the same server or jointly by one or more of the organizations identified  
30 above.

15 The method according to the present invention can include the following steps:

35 The consumer or customer can use the client system to establish a connection with the  
server system. If the client system does not have a unique key and thus is not registered  
with the server system (and the owner, distributor or retailer), the client system and server  
40 system interact to enable the consumer to register with the distributor or retailer such as  
providing the customer name, address, telephone and even credit card information. The  
20 server system generates a unique key for the client system and transmits the unique key to  
the client system to use in connection with transactions with the server system.  
45 Preferably, the unique key is embedded into the software and/or hardware which makes  
up part of the client system, and is transmitted or delivered to the consumer. The client  
50 system which contains the unique key is now used in all subsequent transactions with the  
25

5 distributor or retailer server. The consumer uses the client system to purchase a work  
such as a song or group of songs, such as an album, from the distributor or a product or  
service from a retailer. Because the client system has a unique key, the client system can  
10 be used to enter into an electronic transaction with the distributor or retailer by simply  
5 selecting the work or the good or service desired from a list, such as a menu or a web  
15 page, and manifesting an intent to enter into the transaction, such as by clicking on a  
button, typing a letter or word or transmitting information (such as credit/debit card or  
account information) to the server system. Once the consumer manifests the intent to  
20 enter into the transaction, the act can be recorded by the server system and the server  
10 system can utilize the electronic commerce system to affect the transfer of value to the  
25 appropriate parties or the server system. If the value is successfully transferred, the  
server system can encrypt the work using the consumer's unique key and transmit the  
work to the client system or in the case of hard goods or services, interact with other  
30 systems to cause the goods or services to be delivered to the consumer. In an alternative  
15 embodiment, the method and system of the invention can use a public key encryption  
35 system in which the server system uses the consumer's public key to encrypt the work to  
be transmitted to the client system and the client system uses the client's private key to  
decrypt and use and enjoy the work.

#### 40 20 BRIEF DESCRIPTION OF THE DRAWINGS

45 The foregoing and other objects of this invention, the various features thereof, as  
well as the invention itself, may be more fully understood from the following description,  
when read together with the accompanying drawings in which:

50 FIGURE 1 is a diagrammatic view of a system for distributing works over a  
25 network according to the present invention;

FIGURE 2 is a diagrammatic view of an alternate system for distributing works over a network according to the present invention;

FIGURE 3 is a diagrammatic view of a method of operating a media server in accordance with the present invention;

FIGURE 4 is a diagrammatic view of a method of distributing low quality copies of a work according to the present invention;

FIGURE 5 is a diagrammatic view of a method of distributing high quality copies of a work according to the present invention;

FIGURE 6 is a diagrammatic view of a method of using a media player to decrypt and play an encrypted work according to the present invention;

FIGURE 7 is a diagrammatic view of a method of searching a database for a work according to the present invention;

FIGURE 8 is a diagrammatic view of a method of demonstrating a low quality copy of a work according to the present invention;

FIGURE 9 is a diagrammatic view of a method of downloading a high quality copy of a work according to the present invention;

FIGURE 10 is a diagrammatic view of method of purchasing a copy of a work according to the present invention;

FIGURE 11 is a diagrammatic view of a method of uploading music to a distribution server according to the present invention;

FIGURE 12 is a diagrammatic view of a method of transferring value in exchange for the receipt of a work according to the present invention;

FIGURE 13 is a diagrammatic view of a method of registering a client system with a server system according to the present invention;

10  
5           FIGURE 14 is a diagrammatic view of method of browsing a server system database to select a work according to the present invention; and

10           FIGURE 15 is a diagrammatic view of a universal electronic commerce for distributing works and conducting electronic transactions for the sale of goods and  
5           services over a network according to the present invention.

15           DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

          The present invention is directed to a method and system for conducting secure electronic commerce transactions. In order to illustrate the application of the invention  
20           and to facilitate a better understanding of the invention, the invention is described below as embodied in a method and system for distributing music over a network such as the  
10           internet. While the invention is suited for distributing copyrightable works (such as, for  
25           example, music, audio, video and text) in electronic form, a person having ordinary skill in the art will appreciate, the invention can be embodied in a method and system for  
30           conducting electronic commerce such as retail sales over a network.

15           The method and system according to the invention allow customers to browse a list of music, listen to a preview, and purchase a copy of encoded music files (such as MP3  
35           encoded files) over the Internet. In accordance with the invention, three components can be used to accomplish this task: 1) a Media Server; 2) a Remote or client system (customer); and 3) a website and associated backend system. In one embodiment, the  
40           media server is primarily responsible for distributing music to users across the Internet. In this embodiment, the system server can be a physical machine connected to the Internet  
45           and the media server can include a computer program software that runs on one or more system servers. The remote or client system can include any device (such as, a computer, personal digital assistant or portable MP3 player) that can be used for searching, playing,  
50           and purchasing music. The web site has a multi-purpose role. The web site is used for  
25

11  
5 database maintenance and searching, credit card processing, and song playback. Each of these components utilize a database of information centrally stored on the system servers.

10 Figure 1 shows a system 100 for distributing music over a network such as the internet 105 in accordance with the present invention. The system 100 includes a media  
15 web server 110 such a Unix or LINUX based web server, for example Slackware Linux, installed on an Intel Corp. (Santa Clara, CA) or Digital Equipment Corporation/Compaq (Houston, TX) or Sun Microsystems SPARC (Palo Alto, CA) based computer 112. The  
20 media web server 110 is connected to the internet 105, for example by a T1 connection. The media web server 110 can include a database 114, such as a SQL compatible database  
10 created by MySQL available from T.C.X DataKonsult AB of Stockholm, Sweden. The media web server 110 can include a media server engine 112 which includes software  
25 which enables the media web server to distribute encoded music. The media web server 110 can include an electronic commerce engine 116, such a CyberCash CashRegister  
30 Payment Services available from CyberCash, Inc. of Reston, Virginia. The media web  
15 server 110 can further include an encoding/decoding engine such as an MPEG encoding/decoding engine for converting audio such as music to various levels of quality  
35 and an encryption engine for generating unique keys and encrypting music streams to be downloaded by the client. One such MPEG encoding/decoding engine is Xaudio available  
40 from MPEGTV of San Francisco, California. One such encryption/decryption engine is BlowFish available from Counterpane Systems of Minneapolis, Minnesota. Another  
20 encryption/decryption engine can be a public key - private key system such as Pretty Good Privacy available from Network Associates, Inc. of Santa Clara, California.

45 The system 100 can also include a customer computer system 120 to enable the customer/consumer to transfer payment to the distributor or owner and download music,  
50 videos or text. The customer computer system 120 can be any personal computer 122,  
25



5 such as an Apple MacIntosh or an IBM compatible personal computer. In one  
embodiment, the customer computer system 120 is an IBM compatible personal computer  
10 running the Windows operating system available from Microsoft Corp., Redmond,  
Washington. The customer computer system 120 can also include Netscape  
5 Communicator or Microsoft Internet Explorer as the browser software used to access the  
web site on the Media Web Server 110. The browser can be equipped with a media  
15 player "plug-in" software module or media player computer program or applet 124 which  
can decrypt and decode the encrypted, MP3 encoded work (music, video or text stream) to  
20 allow the user to utilize the work. Alternatively, the media player 124 can be a stand  
10 alone application that can be enabled to access the Media Web Server 110 via the internet  
to browse a list of songs (videos or texts) available for download and complete the  
25 electronic transaction.

The system 100 can further include an author/artist system 130 which can permit  
30 an author, artist, musician or owner of a work to upload a work to the media web server  
15 110. This function can be incorporated in the media player 124 on the same system that is  
used by the customer as discussed above or can be a separate component that is installed  
35 on separate client system 230. Like the customer client system 120, the author/artist  
system 130 can be any computer, such as an Apple MacIntosh or an IBM compatible  
40 personal computer 132.

20 Figure 2 shows an alternative system 200 for distributing music (audio, video or  
text) over the internet in accordance with the present invention. In this embodiment, the  
45 functions of the media web server described above can be distributed over several server  
systems 210 and 211. For example, the an incoming media server 211 can be provided  
for uploading works such as music, videos and text to a common database 214 and an  
50 outgoing media web server 210 can be provided for distributing low quality music (for  
25

13

5 browsing) and high quality music (for purchases) to customers. The outgoing media  
server 210 can include a media server engine 212 to distribute music and an electronic  
commerce engine 216 to facilitate electronic transactions. The outgoing media server 210  
10 can also include the encryption engine 218 and a key database which allows the high  
5 quality music to be encrypted prior to being transferred to the customer system 220 to  
15 prevent unauthorized distribution of the music.

In accordance with one embodiment of the invention, the media server is a central  
element of the system. The media server is primarily responsible for distributing music to  
20 users of the system. The media server can run on one or more system servers connected  
10 to the Internet. The media server is continuously running; it waits for requests from  
remote clients at customer systems and then processes those requests. In accordance with  
25 the inventions, there are two types of download requests the media server acts upon: (1) a  
request for a low quality stream, and (2) a request for a high quality stream. Both  
30 processes are handled in a similar manner, but an additional step is required for a high  
15 quality stream.

As shown in FIGURE 3, when the media server program loads, it enters the ready  
35 state at step 310 and begins listening for requests on a predefined port, such as, for  
example port 3005. Whenever a remote client requests a stream, the request is received at  
40 port 3005 on the system server for processing by the media server at step 312. Upon  
20 receipt of a request, the media server determines whether the received request is a request  
to browse or preview a song (low quality) or a request to purchase a song (high quality) at  
45 step 314. Depending upon whether the request is a request for a high quality stream or a  
low quality stream, the media server will initiate a process to transmit a high quality  
stream at step 316 or a low quality stream at step 318. Typically, the media server will  
50 begin a new process to handle the client (the remote) individually. This new process will  
25

14

5 connect back to the remote on a different predefined port, such as, for example, port 3006  
to handle the data stream. This design allows for the media server to handle simultaneous  
streams without any interference between them. The media server seems to be limited  
10 only by the available hardware.

5 As shown in FIGURE 4, when a remote client requests a low quality media stream  
(a browse), the media server responds by creating a new process to serve the request at  
15 step 412. This process identifies the stream requested and opens the appropriate low  
quality file on the server at step 414. The media server then begins to send the file in  
20 packets across the Internet to the remote client at step 416. This process continues  
10 sending packets until either the end of the file is reached, or the connection to the remote  
client is lost at step 418. When the process terminates at step 420, it returns the media  
25 server to its previous state.

As shown in FIGURE 5, when a remote client requests a high quality stream (a  
30 purchase), the server reacts responds in a similar manner. The server again creates a new  
15 process to handle the request at step 512. Because this file will be written to disk for  
multiple playbacks, the file is opened at step 514 and the file is encrypted so it can not be  
35 distributed after it has been purchased. This is accomplished by using the unique  
registration or key number assigned to the remote client. This information is then used to  
40 encrypt the file as it is being sent to the customer in step 516. Again, the process  
20 continues until the entire file has been sent to the remote client at step 518. After the  
process is finished, it returns the server to its previous state at step 520.

45 The remote client can be a program that resides on the user's computer. The  
remote client can include the functionality to play MPEG or any other encoded music file,  
search the music database at the website, request music streams from the media server,  
50 and allows purchasing of music. Except for the playback of local (on the hard drive)  
25

15

5 MPEG music files, all other processes require an Internet connection to communicate with the servers. There are two types of the remote client: (1) a basic player client which is limited by not allowing the purchase of songs, and (2) a registered player client which has all of the functionality required to use purchase and upload music to the system servers.

10 After a user has downloaded the basic player client, they can register the client. This registration process is performed through the web site, and provides the information needed to process transactions (transfer value), and assigns a unique key to be used in the encryption and decryption process for purchased music. When a user has completed the registration process, a custom version of the registered player client is downloaded to the user's computer.

25 Song playback is handled by song lists at the remote client. A customer can create custom song lists from low quality streams, purchased songs, and any non-encrypted audio file on the customer's computer. As shown in FIGURE 6, when a song is played, the remote client checks to see if the file is a local file at step 612 and if so, the remote client opens the file at step 622, and passes it to the MPEG decoder. The decoder takes the file and decompresses it for playback, and then plays it. If the song is a purchased audio file at step 618, the file is first decrypted at step 620 and then passed to the decoder at step 622. If the file is not a local file at step 612, the remote client initializes a process to download a low quality stream at step 614. In one embodiment, the MPEG encoder/decoder is the X audio MPEG audio engine available from MPEGTV, LLC of San Francisco, California.

45 The song lists used by the remote client can be created from local files, or streams from the system server. As shown in FIGURE 7, when a customer wishes to add a stream to the song list, the information needed to play the song is retrieved through a search of the database. When a customer enters a query, by band name for example, the

16

5 remote client must pass the request to the system server. The remote client connects to the system server at step 712 and passes the request to the system database at 714. The database then performs the search and passes the information back to the remote client  
10 where the information can be added to the song list at step 716 before closing the connection at step 718.

15 As shown in FIGURE 8, when a user requests a low quality stream (a browse) from the media server at step 812, the media server can establish a separate connection to the remote client for the purpose of transmitting the music data to the remote client. As the remote client receives the information from the media server, it is passed to the MPEG  
20 decoder at step 814 for playback. At this point the stream is treated as if it were a local file. As the information is retrieved from the media server, it is stored in memory. The information is never written to disk because it is intended that the song will not be stored permanently on the user's machine. In one embodiment, the low quality stream is a  
25 24Kb/s, 22KHz MP3 encoded stream or lower quality.

15 A shown in FIGURE 9, when a customer requests a high quality stream (a purchase) at step 918 from the media server, the process is similar to a browse. A high quality stream is initiated in step 912 and the song is downloaded. A purchased song is  
35 not played as it is downloaded. Because the file is purchased, the file is stored in its encrypted form on the memory of the customer's system in step 914. This allows the customer to listen to the file without the need to be connected to the Internet. In one  
40 embodiment, the high quality stream is a 128kb/s, 44.1KHz MP3 encoded stream or better quality.

As shown in FIGURE 10, customers can purchase songs with the remote client. Customers must first purchase points from the web site before purchasing songs. When a  
50 customer buys a high quality sound file, the remote handles the transaction. A connection  
25

55

17

5 is established to the database on the system server in step 1012. The remote client checks  
the database for points to purchase the song at step 1014. If a customer has points  
available at step 1016, the number of points is automatically updated in the database at  
10 step 1020, the database connection is closed at step 1022, and the remote client initiates a  
5 high quality stream from the media server at step 1024. If the customer doesn't have  
enough points at step 1016, the customer is informed of the deficiency and the process is  
15 terminated at step 1018.

As shown in FIGURE 11, musicians can upload their music to the database using  
20 the remote client. The musician needs only a high quality audio file such as a 128 kb/s,  
10 44.1 kHz, Stereo MP3 file and a musician account in the database. A musician account  
can be created on the web site by a registered customer. When the process begins, the  
25 musician can be prompted to select the items to be uploaded at step 1110 and to input  
information about the song at step 1112. This information can be stored and later used in  
searches of the database. The remote client then connects to the database at step 1114,  
30 updates the information in the database at step 1116, and uploads the file to the system  
server at step 1118. After the song upload is complete, the database connection is closed  
35 at step 1120. Once the file is saved on the server, a separate process can be used to create  
the low quality file at step 1122. For example, the high quality file is decoded into .wav  
40 format, then encoded into a low quality (24 kb/s, 22 kHz, Stereo) MP3 and saved. The  
20 song will be available once it has been checked for errors.

The web site provides a range of functionality to both customers and musicians.  
45 Some of the functions the web site can perform are: (1) To collect a variety of user  
information, (2) Credit card processing, (3) Client registration, and (4) Generating listings  
from search of the database. Information can be collected throughout the web site using  
50 HTML forms and stored in the database. Credit card processing can be handled through a  
25

18

5 3<sup>rd</sup> party service, such as cyber cash payment services available from Cyber Cash, Inc.,  
Reston, Virginia. Client registration provides the customer with a fully functional remote  
client that can be used to purchase music. The band information features, musician listings  
10 and musician information, rely on querying the database for information, and presenting it  
5 to the user.

15 One portion of the e-commerce system is credit card processing. As shown in  
FIGURE 12, when the customer purchases points, the customer must select a payment  
method at step 1210 and enter the transaction information such as credit card information  
20 to complete the transaction at step 1212. Points can be used to purchase songs. The  
10 number of points a user currently has is tracked in the database. Unlike the rest of the web  
site, the credit card processing pages use secure sockets (SSL) to handle the  
25 communications. The web site sends the appropriate information to a 3<sup>rd</sup> party service for  
authentication at step 1214. When a response is received from the authentication service,  
30 if the transaction is approved at step 1216, the program updates the database at step 1220  
15 and if the transaction is not approved, and informs the user of the result of the transaction.

35 Although a customer can browse music and play MP3 files with the basic remote  
client, a customer must have a registered remote client to purchase high quality files. As  
shown in FIGURE 13, when a customer wishes to register at step 1310, they provide  
40 general information about themselves for use by the distribution source at step 1312.  
20 After this information is stored in the database at step 1314, a unique key is assigned to  
the customer for use in the encryption and decryption process of the high quality sound  
45 files at step 1316. A custom registered remote client program is then created with the  
appropriate registration information and sent to the customer at step 1318. A customer  
50 can now purchase high quality sound files and listen to them.

55

5 The artist and band listings provide the customer with the ability to locate artists  
and bands based upon a variety of criteria. The artist/band listing is maintained by the  
website backend. When a search is passed to the backend, it first establishes a connection  
10 to the database. When the connection is established, the backend sends the request to the  
5 database and waits for a response. As the information is returned from the database, it is  
15 formatted according to template files. These templates provide instructions for how the  
information is formatted in standard HTML. The generation of artist/band listings can be  
initiated by: (1) custom searches of the database from the web site, or (2) changes to the  
20 database.

10 In addition, as shown in FIGURE 14, a customer can also initialize a browse  
function from the web site at step 1410. When a customer selects a song from the web  
25 page, the web backend sends a file associated with the remote to the user's web browser at  
step 1412. When the web browser receives this file, it automatically launches the remote  
client at step 1414. This file contains instructions that initiate a low quality stream of the  
30 song selected from the web site.  
15

35 Figure 15 shows a system 1500 for conducting electronic commerce over the  
internet in accordance with the present invention. In this embodiment, the system  
includes a plurality of servers 1510, 1520, 1530 and a universal electronic commerce  
40 client 1550. The client 1550 can include a web browser 1554 which is configured to  
20 include a unique encryption key or other unique identifier 1556 which is used for all  
electronic transactions with a retail web server 1530 which allows for the secure purchase  
45 of goods, services or works (audio, video or text). The retail web server 1530 can include  
any computer server coupled to a retailer/distributor database 1532 that is used in  
electronic transactions for the sale of goods, services or the distribution of audio, video or  
50 text works. The system 1500 can also include a key encryption system in which the  
25



20

5 client's unique private key is stored in an independent, trusted public key server 1520 and  
associated key database 1522 which can only accessed by authorized retailer or distributor  
servers. The system 1500 can also include a credit/debit web server 1510 which permits  
10 the customer to establish an account and provides for the transfer of value (payment) in  
exchange for works downloaded. The credit/debit web server 1510 can include a  
15 credit/debit database 1512 in which customer, retailer, distributor and owner accounts can  
be stored.

20 As one of ordinary skill will appreciate, the system of the present invention can be  
used to distribute works (audio, video or text) in a business to business context as well as  
10 a business to consumer or customer context. For example, music can be distributed for  
use in offices, waiting rooms and elevators using the above identified system. In this  
25 embodiment the music can be downloaded as needed based on a predefined program or  
downloaded and stored for later playback according to a predefined program.  
30 Alternatively, the browse mode can be used to receive predefined or random streams of  
15 music for use in offices, waiting rooms or elevators, etc.

35 The invention may be embodied in other specific forms without departing from the  
spirit or essential characteristics thereof. The present embodiments are therefore to be  
considered in respects as illustrative and not restrictive, the scope of the invention being  
40 indicated by the appended claims rather than by the foregoing description, and all changes  
20 which come within the meaning and range of the equivalency of the claims are therefore  
intended to be embraced therein.

## Claims

5

10

15

20

25

30

35

40

45

50

55

What is claimed is

1. An apparatus for distributing a units of information representative of copyrightable works over a network, said apparatus comprising:

an information database adapted for storing said units of information representative

of copyrightable works;

a media server, connected to said information database, including a computer system, associated memory, and media server software, said media server software being adapted to retrieve said units of information from said information database and to transmit said units of information to a plurality of client systems over said network;

an encryption engine connected to said media server and adapted for processing each of said units of information to create encrypted units of information according to a unique key for each client system.

2. A system for distributing a units of information representative of copyrightable works over a network comprising:

an information database adapted for storing said units of information representative of copyrightable works;

a media server, connected to said information database, including a computer system and associated memory, said media server including media server software, said media server software being adapted to retrieve said units of information from said information database and to transmit said units of information to a plurality of client systems over said network;

an encryption engine connected to said media server adapted for processing each of said units of information to create encrypted units of information according to a unique key for each client system;

a client system including a computer system, associated memory, and client

22

software, said client software being adapted for communicating with said media server to receive said encrypted units of information from said media server;

said client system including a reader adapted for decrypting and presenting said information to an end user;

wherein said reader includes a unique key adapted decrypting said encrypted units of information and said media server is adapted for encrypting said units of information according to at least one key that is unique to the reader of each client system.

3. A method of distributing units of information representative of copyrightable works over a network comprising the steps of:

storing each of said units of information in a database;

upon request from a client system for a particular unit of information, retrieving said unit of information and encrypting said unit of information using a key unique to said client system; and

transferring said encrypted unit of information to said client system.

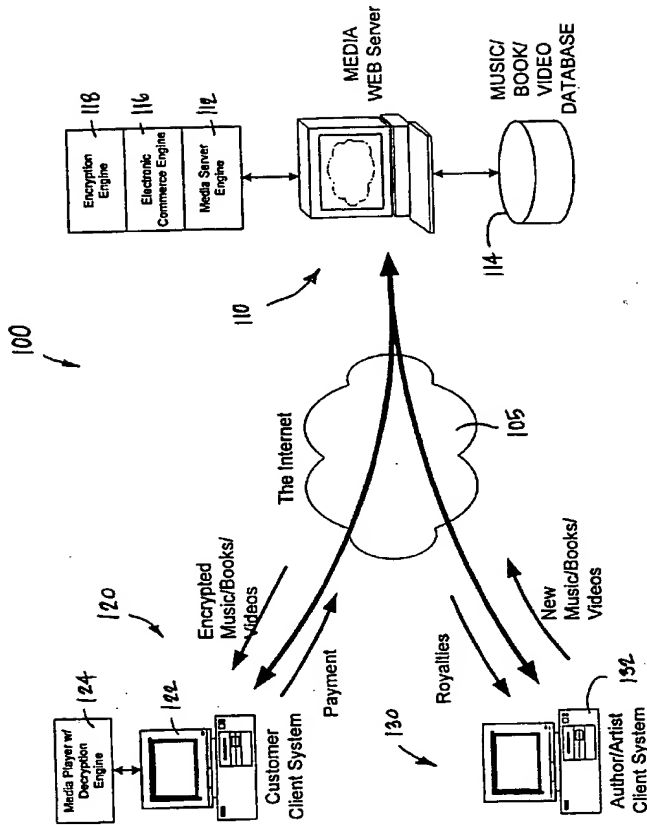


FIG. 1

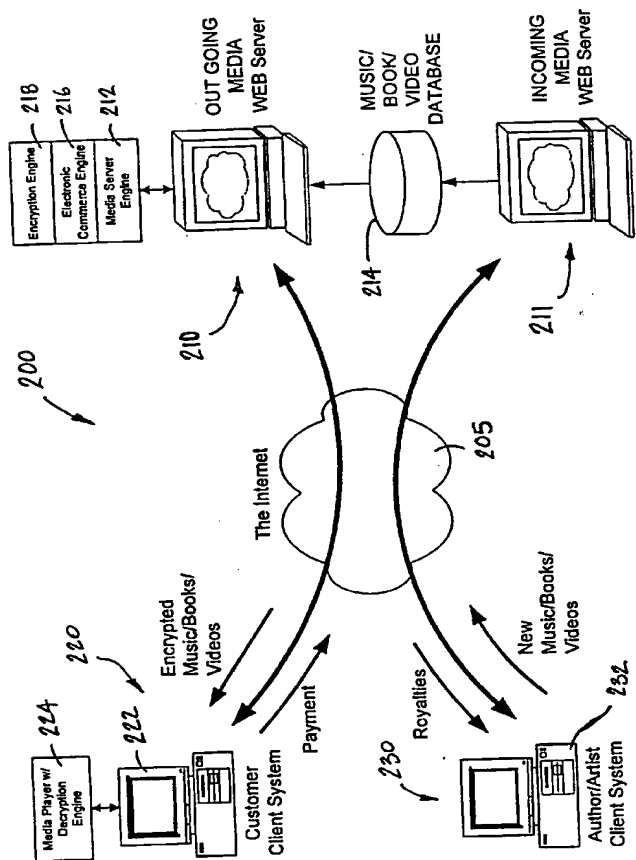
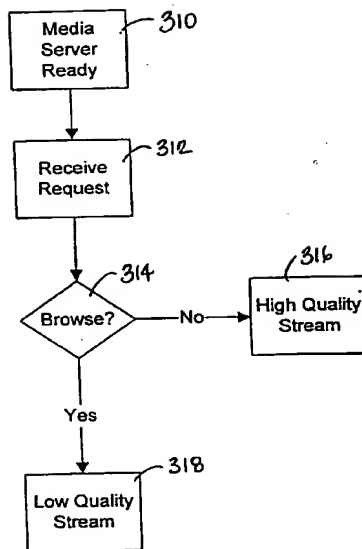
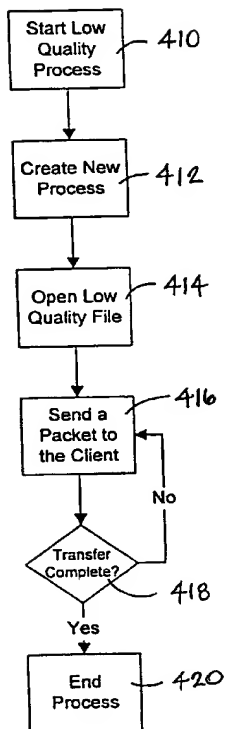


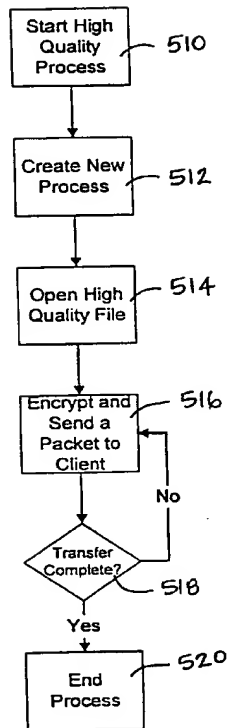
FIG. 2

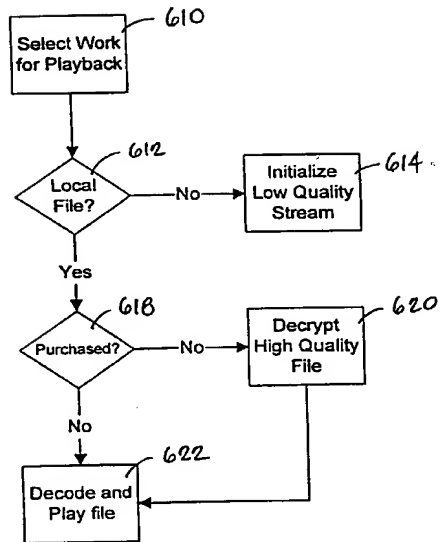
**FIG. 3**

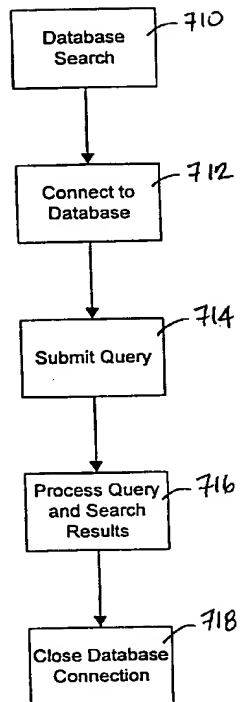
4/15

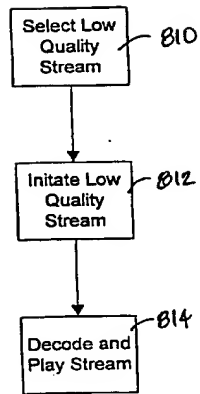
**FIG. 4**



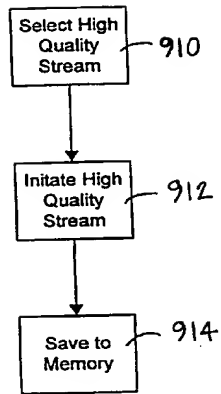
**FIG. 5**

**FIG. 6**

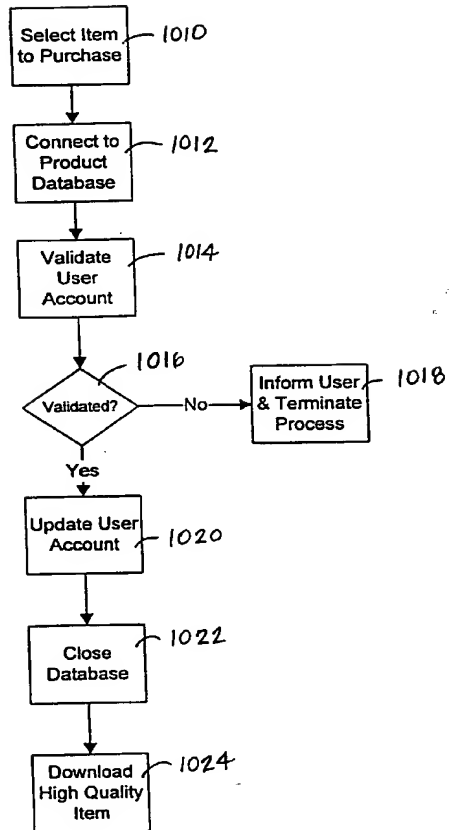
**FIG. 7**

**FIG. 8**

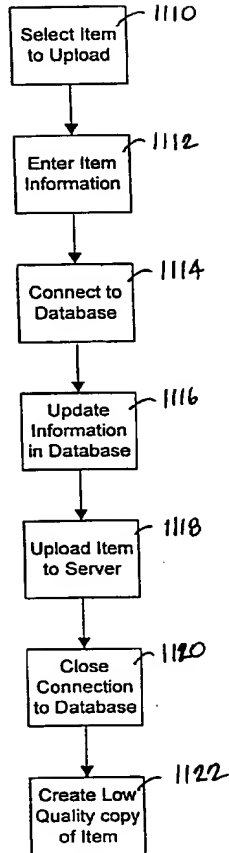
9/15

**FIG. 9**

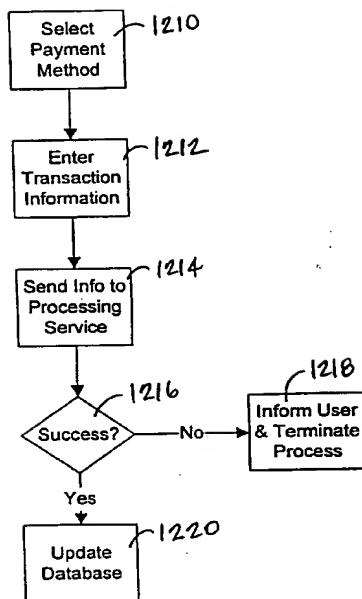
10/15

**FIG. 10**

11/15

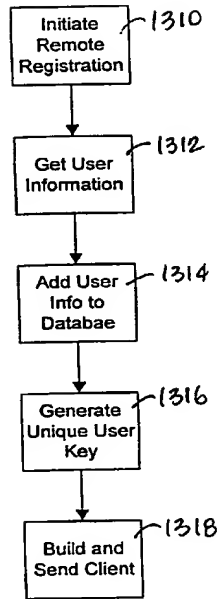
**FIG. 11**

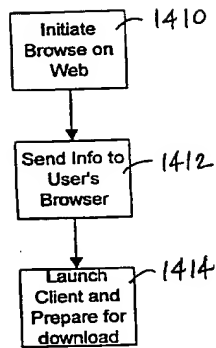
12/15

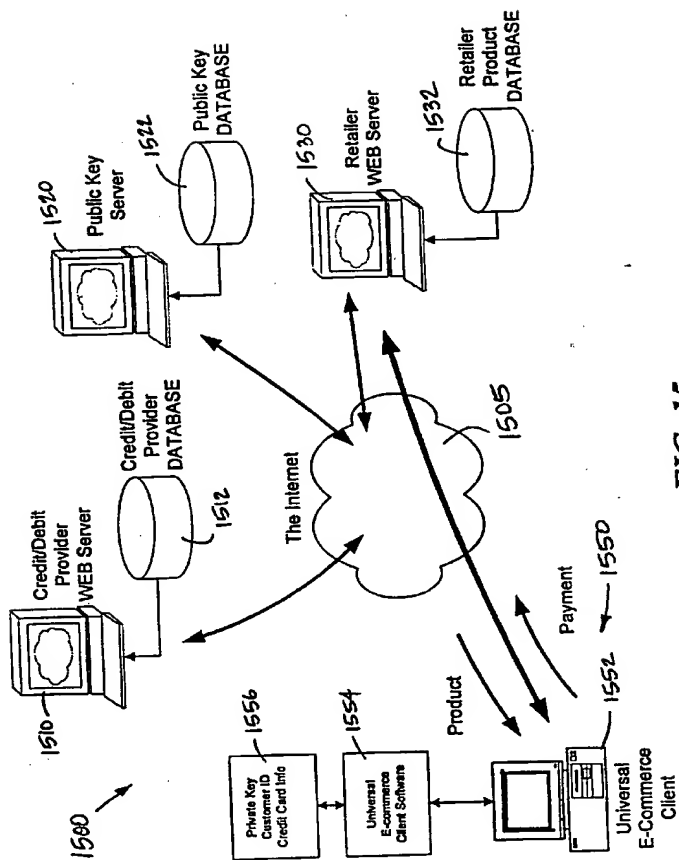
**FIG. 12**



13/15

**FIG. 13**

**FIG. 14**



# INTERNATIONAL SEARCH REPORT

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 G06F17/60 H04L29/06 G06F1/00		Int. Appl. No. PCT/US 00/09774
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC 7 H04L G06F G07F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, PAJ		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 843 449 A (SUNHAWK CORP INC) 20 May 1998 (1998-05-20) column 2, line 12 -column 4, line 5 column 5, line 9 - line 25 column 5, line 53 -column 8, line 19 column 9, line 11 - line 30 column 10, line 30 -column 11, line 36 figures 1,3-5 --- -/-	1-3
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C. <input checked="" type="checkbox"/> Patent family members are listed in annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" documents published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "Z" document member of the same patent family		
Date of the actual completion of the international search 30 August 2000		Date of mailing of the international search report 06/09/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentsaan 2 NL - 2200 HV Rijswijk Tel: (+31-70) 340-2040, Tx. 31 651 aprot, Fax: (+31-70) 340-3018		Authorized officer Carnerero Álvaro, F

Form PCT/ISA/210 (second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Int. Application No.  
PCT/US 00/09774

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHOUDHURY A K ET AL: "COPYRIGHT PROTECTION FOR ELECTRONIC PUBLISHING OVER COMPUTER NETWORKS" IEEE NETWORK: THE MAGAZINE OF COMPUTER COMMUNICATIONS,US,IEEE INC. NEW YORK, vol. 9, no. 3, 1 May 1995 (1995-05-01), pages 12-20, XP000505280 ISSN: 0890-8044 page 14, right-hand column, paragraph 5 -page 18, right-hand column, paragraph 6	1-3
A	BALASUBRAMANIAN R ET AL: "TOWARD OBJECT-WEB BASED SERVICE PROVIDER INFRASTRUCTURE FOR E-COMMERCE TRANSACTIONS" ISS. WORLD TELECOMMUNICATIONS CONGRESS. (INTERNATIONAL SWITCHING SYMPOSIUM),CA,TORONTO, PINNACLE GROUP, 21 September 1997 (1997-09-21), pages 105-112, XP000704461 figures 1,8	1-3
A	NAGASAKA A ET AL: "GENERAL PURPOSE MEDIA SERVER CONFORMING TO DAVIC: OKI MEDIA SERVER V2" OKI TECHNICAL REVIEW,JP,OKI ELECTRIC INDUSTRY, TOKYO, vol. 63, no. 159, 1 July 1997 (1997-07-01), pages 11-16, XP000699912 ISSN: 0912-5566 page 11	1-3
A	ME L ET AL: "LE COMMERCE ELECTRONIQUE: UN ETAT DE L'ART" ANNALES DES TELECOMMUNICATIONS - ANNALES OF TELECOMMUNICATIONS,CH,PRE SSES POLYTECHNIQUES ET UNIVERSITAIRES ROMANDES, LAUSANNE, vol. 53, no. 9/10, 1 September 1998 (1998-09-01), pages 361-376, XP000791619 ISSN: 0003-4347 page 12, right-hand column -page 13, left-hand column	1
A	SOMOGYI S: "MP3: A NEW AUDIO POWER - BUT WHOSE ?" AUDIO,US,AUDIO. PHILADELPHIA, vol. 82, no. 11, November 1998 (1998-11), page 20,22 XP000791991 ISSN: 0004-752X the whole document	1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int'l. Patent Application No.  
PCT/US 00/09774

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0843449 A	20-05-1998	US 5889860 A	30-03-1999
		CA 2220457 A	08-05-1998
		JP 10301904 A	13-11-1998